

SEALED

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of Nebraska

United States of America)

v.)

VYACHESLAV IGOREVICH PENCHUKOV, a/k/a "tank;") Case No.

IVAN VIKTORVICH KLEPIKOV, a/k/a "petrovich;" ALEXEY) 4:12MJ3052

DMITRIEVICH BRON, a/k/a "thehead;")

ALEXEY TIKONOV, a/k/a "kusanagi;" YEVHEN KULIBABA, a/k/a "jonni;")

YURIY KONOVALENKO, a/k/a "jtk0;" JOHN DOE #1, a/k/a "lucky 12345;")

JOHN DOE #2, a/k/a "aqua;" and JOHN DOE #3, a/k/a "mricq")

*Defendant(s)***CRIMINAL COMPLAINT**

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of May 2009 to present in the county of Douglas, Lancaster & Pierce in the
District of Nebraska, the defendant(s) violated:

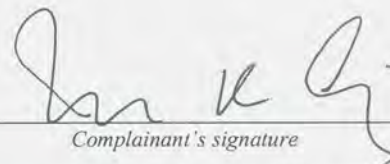
*Code Section**Offense Description*

18 U.S.C. § 1962(d)

See Attachment A to the affidavit, said attachment incorporated herein by reference

This criminal complaint is based on these facts:

See affidavit, said affidavit incorporated herein by reference.

☒ Continued on the attached sheet.

Complainant's signature

James K. Craig, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 7/13/2012 10:15 amCity and state: LINCOLN, NEBRASKA

Judge's signature

CHERYL R. ZWART, U.S. MAGISTRATE JUDGE

Printed name and title

ATTACHMENT A

Offense description

From in or about May 2009, and continuing to the present, in the District of Nebraska and elsewhere, VYACHESLAV IGOREVICH PENCHUKOV, IVAN VIKTORVICH KLEPIKOV, ALEXEY DMITRIEVICH BRON, ALEXEY TIKONOV, YEVHEN KULIBABA, YURIY KONOVALENKO, JOHN DOE #1, JOHN DOE #2, and JOHN DOE #3 (hereinafter “DEFENDANTS”), each being a person employed by and associated with the Jabber Zeus Crew, an enterprise engaged in, and the activities of which affected, interstate and foreign commerce, together with others known and unknown, did knowingly and intentionally conspire to violate 18 U.S.C. § 1962(c), that is, to conduct and participate, directly and indirectly, in the conduct of the affairs of the enterprise through a pattern of racketeering activity, as defined in 18 U.S.C. §§ 1961(1) & (5), which pattern of racketeering activity consisted of multiple acts indictable under 18 U.S.C. § 1344 (bank fraud) and 18 U.S.C. § 1028 (identity theft). It was a further part of the conspiracy that each defendant agreed that a conspirator would commit at least two acts of racketeering activity in the conduct of the affairs of the enterprise.

In violation of Section 1962(d) of Title 18 of the United States Code.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA,

Plaintiff,

v.

VYACHESLAV IGOREVICH
PENCHUKOV,

also known as "tank;"

IVAN VIKTORVICH KLEPIKOV,

also known as "petr0vich;"

ALEXEY DMITRIEVICH BRON,

also known as "thehead;"

ALEXEY TIKONOV,

also known as "kusanagi;"

YEVHEN KULIBABA,

also known as "jonni;"

YURIY KONOVALENKO,

also known as "jtk0;"

JOHN DOE #1, also known as "lucky12345;"

JOHN DOE #2, also known as "aqua;"

JOHN DOE #3, also known as "mricq;"

Defendants.

Case No. _____

UNDER SEAL

AFFIDAVIT IN SUPPORT OF COMPLAINT

I, Special Agent James K. Craig, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a criminal complaint against VYACHESLAV IGOREVICH PENCHUKOV, IVAN VIKTORVICH KLEPIKOV, ALEXEY DMITRIEVICH BRON, ALEXEY TIKONOV, YEVHEN KULIBABA, YURIY KONOVALENKO, JOHN DOE #1, also known as "lucky12345," JOHN DOE #2, also known as "aqua," and JOHN DOE #3, also known as "mricq," (hereinafter, the "DEFENDANTS").

2. I am a Special Agent with the FBI and have been since August of 2008. Relative to this investigation, since July of 2009, my duties include the investigation of offences including violation of Title 18, United States Code, Section 1030, unauthorized access to computers and computer fraud. I have received specialized training for conducting computer-based investigations, including training regarding computer hardware, networks, network security and computer intrusions. I have received training from the FBI regarding computer crimes and have extensive experience regarding computers, networks and the workings of the Internet.

3. I am presently employed as a Special Agent of the Federal Bureau of Investigation (FBI), and am assigned to the Cyber Crime Task Force of the Omaha Field Office in the District of Nebraska. I have been employed by the FBI since August 2005, and have been a Special Agent since August 2008.

4. The information contained in this affidavit is based upon my personal knowledge, my review of documents and other evidence, my conversations with other law enforcement officers and other individuals, and my training and experience. All conversations and statements described in this affidavit are related in substance and in part unless otherwise indicated. Because this affidavit is being submitted for the limited purpose of establishing probable cause, I have not included every detail of every aspect of the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause. I have not, however, excluded any information known to me that would defeat a determination of probable cause.

PROBABLE CAUSE

A. Overview

5. This affidavit establishes probable cause to believe that DEFENDANTS are participating in a conspiracy to conduct and participate, directly and indirectly, in the conduct of the affairs of an enterprise through a pattern of racketeering activity, as defined in 18 U.S.C. §§ 1961(1) & (5), which pattern of racketeering activity consisted of multiple acts indictable under 18 U.S.C. § 1344 (bank fraud) and 18 U.S.C. § 1028 (identity theft). Specifically, the DEFENDANTS and others have conspired to employ widespread computer intrusion, malicious software, and fraud to steal millions of dollars from several bank accounts in the United States and elsewhere. As more fully described below, DEFENDANTS and others have infected thousands of business computers with malicious software that captures passwords, account numbers, and other information necessary to log into online banking accounts, and have then used the captured information to steal millions of dollars from victims' bank accounts.

B. Defendants

6. At all times material to this affidavit:
 - a. VYACHESLAV IGOREVICH PENCHUKOV was a resident of Ukraine. He used the online nickname "tank." PENCHUKOV coordinated the exchange of stolen banking credentials and money mules. PENCHUKOV also received alert messages which provide notification once a bank account has been compromised.
 - b. IVAN VIKTORVICH KLEPIKOV was a resident of Ukraine. He used the online nickname "petr0vich." KLEPIKOV was a systems administrator who handled the technical aspects of the criminal scheme. KLEPIKOV also received alerts which

provided notification once a bank account has been compromised.

- c. ALEXEY DMITRIEVICH BRON was a resident of Ukraine. He used the online nickname “thehead.” BRON was the financial manager of the criminal operations. BRON managed the transfer of money through an online money system known as Webmoney.
- d. ALEXEY TIKONOV was a resident of Russia. He used the online nickname “kusanagi.” TIKONOV was a coder or developer who assisted the criminal enterprise by developing new codes to compromise the banking systems.
- e. YEVHEN KULIBABA was a resident of the United Kingdom. He used the online nickname “jonni.” KULIBABA, who is in custody in the United Kingdom, provided money mules and their associated banking credentials in order to facilitate the movement of money which is withdrawn from victim accounts by fraudulent means. He operated the money laundering network in the United Kingdom.
- f. YURIY KONOVALENKO was a resident of the United Kingdom. He used the online nickname “jtk0.” KONOVALENKO, who is in custody in the United Kingdom, provided money mules’ and victims’ banking credentials to KULIBABA and facilitated the collection of victim data from other conspirators.
- g. JOHN DOE #1 was a resident of Russia. He used the online nickname “lucky12345.” “Lucky12345” was a coder who developed new codes to compromise the banking system and assists others in stealing and exploiting banking credentials.
- h. JOHN DOE #2 was a resident of Russia. He used the online nickname “aqua.”

“Aqua” provided money mules and their associated banking credentials in order to facilitate the movement of money which is withdrawn from victim accounts by fraudulent means.

- i. JOHN DOE #3 was a resident of Ukraine. He used the online nickname “mricq.” “Mricq” was a coder who developed new codes to compromise the banking system and passed user credentials to other conspirators.

C. Selected Victims

7. At all times material to this affidavit:
 - a. BANK OF AMERICA was a financial institution insured by the Federal Deposit Insurance Corporation, and was headquartered in Charlotte, North Carolina.
 - b. BULLITT COUNTY FISCAL COURT was a municipal government office in Shepherdsville, Kentucky.
 - c. DOLL DISTRIBUTING was a business located in Des Moines, Iowa.
 - d. FIRST FEDERAL SAVINGS BANK was a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Elizabethtown, Kentucky.
 - e. FIRST NATIONAL BANK OF OMAHA was a financial institution insured by the Federal Deposit Insurance Corporation, and was headquartered in Omaha, Nebraska. It offered online banking services through computer servers located in Nebraska.
 - f. FRANCISCAN SISTERS OF CHICAGO was a religious congregation headquartered in Homewood, Illinois.

- g. HUSKER AG, LLC was a business located in Plainview, Nebraska.
- h. KEY BANK was a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Sylvania, Ohio.
- i. ODAT LLC, doing business as AIR TREATMENT COMPANY, was a business located in Clifton, Virginia.
- j. PARAGO, INC. was a business located in Lewisville, Texas.
- k. SALISBURY BANK & TRUST was a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Salisbury, Massachusetts.
- l. TOWN OF EGREMONT was a town in Massachusetts with its own municipal government.
- m. UNION BANK AND TRUST was a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Lincoln, Nebraska.
- n. UNION BANKSHARES CORPORATION was a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Ruther Glen, Virginia.
- o. UNITED DAIRY, INC. was a business located in Martins Ferry, Ohio.

D. The Enterprise

8. The DEFENDANTS and others known and unknown (collectively, the “Jabber Zeus Crew”), constituted an “enterprise” as defined in Section 1961(4) of Title 18, United States Code, that is, a group of individuals associated in fact that engaged in, and the activities of which affected, interstate and foreign commerce. The enterprise constituted an ongoing organization whose members functioned as a continuing unit for the common purpose of achieving the objectives of the enterprise.

9. The purposes of the enterprise included the following:
 - a. Infecting the computers used by small businesses and non-profit organizations with malicious software;
 - b. Obtaining bank account numbers, passwords, PIN numbers, RSA SecureID token codes, and similar information necessary to log into online bank accounts;
 - c. Initiating electronic funds transfers from those bank accounts to the bank accounts of “money mules”;
 - d. Transferring funds from money mules to overseas;
 - e. Obtaining the use of computer servers necessary to obtain banking credentials and provide real-time communications among enterprise members; and
 - f. Assigning different members the tasks of writing malicious software, administering computer servers, recruiting money mules, infecting computers, accessing bank accounts to make unauthorized transfers, and receiving transferred funds outside the United States.

E. Electronic Funds Transfer System

10. This investigation has identified numerous unauthorized Electronic Funds Transfers (EFTs) initiated from victim bank accounts. There are two primary types of EFTs: wire transfers, and Automated Clearing House (ACH) payments. Both of these EFTs are performed through the Federal Reserve Bank System. The primary method used by the DEFENDANTS to steal funds has been through Automated Clearing House (ACH) payments.

11. Wire transfers are real-time transfers of funds. After a wire transfer is initiated from a sending bank, the sending bank’s Reserve Account at the Federal Reserve Bank is

immediately debited and the receiving bank's Reserve Account is immediately credited. Wire transfers are typically performed when transactions are time-sensitive or are for large dollar amounts. Recipients of wire transfers have immediate access to the funds through their account at the receiving financial institution.

12. ACH Payments are made through the ACH Network, which is a batch-oriented EFT system wherein batch transfers are settled the next day. The ACH Network is governed by the National Automated Clearing House Association (NACHA) regulations. The Federal Reserve and Electronic Payments Network act as the central clearing facilities through which institutions transmit or receive funds. ACH Payments are typically used for direct deposit to payroll, direct payment for consumer bills (mortgages, loans, etc.), electronic checks, business-to-business payments, or e-commerce payments. ACH payments are either credits (also known as direct deposits) or debits (also known as direct payments). An ACH credit is always initiated by the sender whereas ACH debits are initiated by either the sender or receiver. ACH Payments are submitted in batches from the originator (through their financial institution) to the Federal Reserve Bank. One day later, these batch payments are settled and the payment is sent to the receiving depository financial institution. At the time of settlement, funds are debited from the sending financial institution's account at the Federal Reserve Bank and credited to the receiving financial institution's account.

13. Larger financial institutions have developed their own software to conduct ACH Payments and wire transfers based on the rules governing EFTs through the Federal Reserve Bank. Smaller financial institutions that do not have their own Information Systems Departments utilize Third-Party Processor systems, which allow these banks to conduct EFTs. There are several companies which have developed systems which are utilized by these smaller

financial institutions to conduct EFTs, including FundsXpress, Fiserv, FundTech, CashEdge, Jack Henry, and Metavante. Each of these companies must comply with same regulations that the financial institutions are required to follow. FundsXpress, which is a subsidiary of First Data, has approximately 600 client financial institutions for which it processes EFTs. This investigation has uncovered fraudulent EFTs which were processed through several Third-Party Processors.

F. The Zeus Malware

14. FirstData ("FD") requires all client financial institutions to provide multi-factor authentication for their banking customers in order to conduct Internet-based banking transactions. This multi-factor authentication uses a username, password, and either a security challenge question or a one-time personal identification number (PIN). The one-time PINs are mailed to the banking customers for later use. FD also uses electronic behavioral analysis in the login authentication process. For example, for each online login attempt, FD stores the customer's IP address, Internet browser, cookie, time of day, and frequency of use to build a profile of the user's activity. If the login behavior differs from their "normal" use, the user is challenged to either enter a one-time PIN or else answer a security question. Therefore, an unauthorized user who attempts to log into the system must not only have the username and password, but the answer to various security questions or the one-time PIN.

15. Beginning in May 2009, the FBI began receiving numerous complaints of fraudulent ACH transfers. Through techniques described later in this affidavit, the FBI was able to determine that a large number of fraudulent transfers were being made by unauthorized users, who were gaining the one-time PINs and security questions in real-time to initiate the transfers.

FBI Omaha, the FBI's Cyber Division, and several other FBI Division offices began coordinating with Internet security researchers, ACH payment processors, and financial institutions in an effort to determine how the unauthorized users were gaining the one-time PINs and security questions in real-time and initiated an effort to determine links between incidents nationwide.

16. On June 1, 2009, Internet security researchers at the company iDefense, a provider of computer security intelligence to corporate clients, discovered a modified version of the "Zeus" malicious software that was capable of sending one-time passwords, such as one-time PINs, directly to the attackers in real-time, through an "instant message" protocol known as Jabber. Based on my training and experience, I know that "Jabber" is a method of sending and receiving text-based communication sent over the Internet, also referred to as "chat."

17. Based on my training and experience and on information developed during this investigation, I know that "Zeus" is the name of an identified "keylogger" used to steal online banking information. A keylogger is a form of malicious code which are designed to capture the keystrokes of a user on the machine which the keylogger is installed.¹ The primary purpose of a keylogger is to capture the keystrokes for usernames and passwords used to access web sites, e-mail, and other services from the victim computer. Keyloggers are often designed to send the captured keystrokes back to the criminal who installed the keylogger on the victim machine.

¹ Malicious code is a term used to describe any software code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan Horses, backdoors, and malicious active content. It is often installed on a victim computer system via the Internet through spam that contains attachments or through a web site where code is injected to automatically download onto a victim system when it is viewed through a web browser. When it is installed onto a victim computer system to perform malicious activity, it is often referred to as malware.

These captured keystrokes are typically sent over the Internet in regular time intervals from the victim machine to a machine controlled by the criminal. An unknown criminal or group of criminals developed this keylogger as part of a toolkit to sell to other criminals. FBI investigations and Internet security company researchers have identified criminals advertising the toolkit for sale on various Internet forums used by criminals to exchange fraud information. Copies of the toolkit have been obtained for analysis. The developers of Zeus gave the toolkit that name. However, it is often detected by anti-virus software under the name “zbot” (short for “Zeus bot”) or “wsnpoem,” based on a directory name created on the victim machine when it is installed. Zeus is referred to as a toolkit because it contains software which enables a criminal to operate a database for storing captured data, operate a command and control server, and to create new variants of the keylogger which are not detectable by anti-virus programs. Simple changes in the software code will change the signature of the keylogger, thus creating a new variant which is not recognized as a Zeus bot even though it is performing the same function as the previous variant.²

18. Zeus had become such a notorious toolkit that in January 2009, computer security researchers in Switzerland, who are well known to FBI Cyber investigators, had devoted a web site to tracking command and control servers communicating with Zeus bots. Their page is hosted at the URL <https://zeustracker.abuse.ch>. This site is often referred to as the “Zeustracker”

² A bot is a computer that has been compromised by malicious software for use in completing malicious and/or illegal tasks via remote direction. Most users that have a computer acting as a bot are not aware that their computers have been compromised. Compromised computer is synonymous with bot, and either may be used based on context. A larger number of bots, called a bot network or botnet, are typically controlled by one computer called a command and control server. The owner of the command and control server can direct the botnet to initiate a denial of service attack, send spam, operate as proxies (blindly forwarding Internet data), host phishing sites, or participate in other crime.

site. The Zeus bots on victim computers can be configured to communicate to the command and control servers through a domain name, such as kerchon.com, and not by the command and control server's IP address. Therefore, a criminal can easily change the computer on which the domain resides (kerchon.com, in this example) and the infected victim computers will communicate with the criminal's new computer system. The criminal can also send the Zeus bot a software configuration update with a new domain for the Zeus bot to communicate. It is therefore difficult to quantify how many criminals or criminal groups are operating Zeus command and control servers. Since the creation of the zeustracker web site, the researchers have identified approximately 1,000 unique command and control server computers which talk to Zeus bots.

19. Zeus bots use encoded (not humanly readable) configuration files that contain the list of banking/web targets for which that particular bot is programmed to capture information. The security researchers referenced above devote time to decoding the configuration files in order to alert the Internet security community of the current and historical target web sites. Researchers search for the unique alpha-numeric key that will decode the configuration file. The unique alpha-numeric keys can be used to decode multiple configuration files. This indicates a relationship between the Zeus bots for which the configuration files are decoding, meaning there is reason to believe that the Zeus bots were deployed or controlled by the same criminal or criminal group.

20. iDefense released analysis in iDefense report #486471 on June 4, 2009. The analysis revealed that the modified version of Zeus was capable of sending one-time passwords, such as one-time PINs, directly to the attackers in real-time, through the Jabber instant message protocol.

21. Further analysis published by iDefense stated that stolen login credentials were sent via the Jabber instant-message protocol to the domain “incomeet.com,” which was hosted on the IP address 66.199.248.195 (hereinafter the “INCOMEET SERVER”). Further, iDefense advised that once the Zeus keylogger was fully installed on a victim system, it would be detected as having the filename “sdra64.exe,” if the virus was not already removed by an anti-virus program.

G. Investigation and Searches of the INCOMEET SERVER

22. Investigation of the Zeus malware led me to believe that a computer with the IP address 66.199.248.195 was receiving Jabber instant messages containing the usernames, passwords, PIN numbers, and possibly other credentials necessary to log into victims’ bank accounts.

23. An open source address lookup of the IP address 66.199.248.195 on September 17, 2009, revealed that it hosted the domain name incomeet.com. It also revealed that the address corresponded to EZZI.NET. EZZI.NET is a company headquartered at 882 Third Avenue, 9th Floor, Brooklyn, NY 11232. EZZI.NET maintains server computers connected to the Internet. Their customers use those computers to operate servers on the Internet that, in turn, provide services to client computers. In general, customers configure their computers remotely, connecting to them over the Internet through the Secure Shell (“SSH”) protocol.

24. On September 18, 2009, an FBI agent interviewed Mohammed Salim, an employee at EZZI.NET. According to Mr. Salim, the INCOMEET SERVER was built by EZZI.NET at the request of the customer, to the customer’s specification. The INCOMEET SERVER has one 500 gigabyte hard drive, 2 gigabytes of RAM, and a dual-core AMD processor. It runs the CentOS 5.0 distribution of the Linux operating system. It was leased to

someone who identified himself as "Alexey S." (no full last name known), who claimed to be associated with a company "IP-Server Ltd," supposedly located at Komsomolskaya St. 1, Moscow, Russian Federation.

25. Pursuant to search warrants, the FBI has searched the INCOMEET SERVER on four occasions: September 28, 2009, December 9, 2009, March 17, 2010, and May 21, 2010.

26. On the INCOMEET SERVER, agents found extensive logs of chat communications. These included usernames, passwords, and temporary token numbers for hundreds of bank and brokerage accounts, username and passwords for Paypal.com and other financial sites, and other information collected from infected victim computers.

27. For example, on March 16, 2010, alone, 16 different Jabber communications that appeared to pertain to stolen banking credentials were passed through the INCOMEET SERVER. Many of these pertained to the same victims. For example, one of those messages read as follows:

```
Panel: http://193.104.41.131/
Template: WebCashMgmt
Added: 2010-03-15 23:48:09
Updated: 2010-03-15 23:48:09
IPv4: 76.79.206.130
BotID:
BotNet:
Country: US
Host: rrcs-76-79-206-130.west.biz.rr.com
UserAgent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR
1.1.4322; AskTB5.6)
Location: https://bob.sovereignbank.com/wcmfd/wcmpw/CustomerLogin
Status: Waitoperator
Data:
Customer/Organization ID: KUS2761
User ID: sysadmin
Password: Kunal[remainder of password redacted]
```

28. From my review of other messages sent through the server, I know that this message represents the transmission of compromised banking credentials. Specifically, this says

that a user with user ID “KUS2761,” and a password beginning “Kunal” (the remainder of the password was in the original message but has been redacted from this affidavit) used the IP address 76.79.206.130 to attempt to access an account on Sovereign Bank, which is in the United States.

29. Additionally, the INCOMEET SERVER contained evidence that it was used by the conspirators to communicate with each other. The INCOMEET SERVER’s operators had configured it to record on its hard drive ongoing logs of every chat message sent through the server. These chat communications included discussions among conspirators made as they were in the progress of transferring money out of victim bank accounts. They also discuss the recruitment of “mules”—persons in the United States who are recruited to receive ACH payments and wire the money outside the United States. They also discuss the operation of their botnet. The conspirators communicated in Russian, using both the Cyrillic and Roman alphabets. All chats quoted in this affidavit have been translated into English, using human translators. In some cases, immaterial lines of chat have been omitted for brevity’s sake.

30. Participants in the chat identified themselves by nicknames. With exceptions, noted below, they do not reveal in chat their real names or other personally identifiable information.

31. On July 2, 2009, a writer for the Washington Post website posted a blog entry titled “PC Invader Costs Ky. County \$415,000,” which began with the lead paragraph, “Cyber criminals based in Ukraine stole \$415,000 from the coffers of Bullitt County, Kentucky this week. The crooks were aided by more than two dozen co-conspirators in the United States, as well as a strain of malicious software capable of defeating online security measures put in place by many banks.” The article generally described the theft of funds from the Bullitt County

Fiscal Court in Shepherdsville, Kentucky, as described in this affidavit. The blog entry is accessible at

http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html.

32. Chat logs show that the conspirators viewed this posting and recognized that it described their criminal activity. For example, the user with the online name of “aqua” said the following to user “tank”: “But they described the entire scheme. The Bastards. They exposed the texts. They laid out the entire scheme. ... It’s necessary to give to the supporting [people?] to read. I’m really pissed. They exposed the entire deal.”

33. Also on July 12, “aqua” and “tank” had this exchange:

tank: Well, nevertheless, they were writing about us.
aqua: So because of whom did they lock Western Union for Ukraine?
aqua: Tough shit.
tank: *****Originator: BULLITT COUNTY FISCAL Company: Bullitt
County Fiscal Court
aqua: So?
aqua: This is the court system.
tank: Shit.
tank: Yes
aqua: This is why they fucked [nailed?] several drops.
tank: Yes, indeed.
aqua: Well, fuck. Hackers: It's true they stole a lot of money.

34. That same day, user “tank,” while chatting with user “indep,” specifically referenced the URL of the Washington Post blog posting and discussed its contents:

tank: [Are you] there?
indep: Yeah.
indep: Greetings.
tank: [http://voices.washingtonpost.com/securityfix/2009/07/
an_odyssey_of_fraud_part_ii.html#more](http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html#more)
tank: This is still about me.
tank: Originator: BULLITT COUNTY FISCAL Company: Bullitt County Fiscal Court

tank: He is the account from which we cashed.
tank: Today someone else send this news.
tank: I'm reading and thinking: Let me take a look at history. For some reason this name is familiar.
tank: I'm on line and I'll look. Ah, here is this shit.
indep: How are you?
tank: Did you get my announcements?
indep: Well, I congratulate [you].
indep: This is just fuck when they write about you in the news.
tank: Whose [What]?
tank: :D
indep: Too much publicity is not needed.
tank: Well, so nobody knows who they are talking about.

35. At roughly the same time that “tank” was having this chat conversation with “indep,” “tank” was also having the following chat conversation with “lucky12345”:

tank: Are you [it] there?
tank: This is what they damn wrote about me.
tank: http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html#more
tank: I'll take a quick look at history
tank: Originator: BULLITT COUNTY FISCAL Company: Bullitt County Fiscal Court
tank: Well, you got [it] from that cash-in.
lucky12345: From 200K?
tank: Well, they are not the right amounts and the cash out from that account was shitty.
tank: Levak was written there.
tank: Because now the entire USA knows about Zeus.
tank: :D
lucky12345: It's fucked.

36. On or about July 29, 2009, DOLL DISTRIBUTING, a company that banks with FIRST NATIONAL BANK OF OMAHA, reported that it experienced two fraudulent ACH payments totaling \$59,222. In a chat message sent on July 28, 2009 from “777” to “hrd” on the INCOMEET SERVER, it was reported that \$29,383 was transmitted from Doll to KODASH CONSULTING, LLC, and that \$29,839 was transmitted to PANDORA SERVICES, LLC.

37. On July 31, 2009, an FBI agent interviewed Renee Michelli, the proprietor of PANDORA SERVICES, LLC. Michelli stated that she been looking for a job and had posted her resume on Internet job seeker sites. She was supposedly “hired” as a United States representative for a Russian software company, “1C.” She was told to establish an LLC with a bank account. She was told her job would involve receiving payments and wiring them outside the United States. On October 2, 2009, Heidi Nelson, the proprietor of KODASH CONSULTING, LLC, was interviewed by another FBI agent. Nelson stated that she lost her job in early 2009, and put her resume on Internet job seeker sites. She was contacted by an individual claiming to be an assistant human resources manager for a Russian company. Her job would be to work with clients in the United States, and on occasion to receive payments from them, which she would transmit to Russia. Based on my training and experience and information developed during this investigation, I believe that Michelli and Nelson were “money mules” hired by the DEFENDANTS to facilitate the transfer of stolen funds.

38. Through the execution of the four search warrants, other agents and I found chat communications on the INCOMEET SERVER describing the transfer of money from a large number of bank accounts, including transfers from bank accounts owned by the Bullitt County Fiscal Court, GCM Federal Credit Union, Doll Distributing, the Town of Egremont, the Franciscan Sisters of Chicago, United Dairy, Inc., Downeast Energy Corporation, Enoch Manufacturing Company, Escrow Source, Inc., Circulation Tools, LLC, Hydro-Pac, Inc., Parago, Inc., Friendship Manor, Bastire Edwards CPAs, and Husker AG, LLC. These chats occurred within hours of the transfers in question. Among other things, the chats were used to transmit log-in credentials for victims, report the transfer of funds to mules, and/or request bank account information for mules. Each of the DEFENDANTS referenced herein participated in one or

more chats relating to or facilitating thefts of log-in credentials or fraudulent transfers of funds from victims. Some of those chats are referenced in Overt Acts, below.

IDENTIFICATION OF THE DEFENDANTS

39. For the reasons set forth below, there is probable cause to believe that the following online nicknames belong to the following defendants:

A. VYACHESLAV IGOREVICH PENCHUKOV, a/k/a “tank”

40. In chat, “tank” reported on July 22, 2009, the birth of his daughter, Miloslava, and gave her birth weight. Ukrainian birth records show one girl born on that day with that name and that birth weight, and VYACHESLAV IGOREVICH PENCHUKOV was her father.

41. Computers seized from PENCHUKOV’s home by Ukrainian authorities (acting pursuant to a Mutual Legal Assistance Treaty request from the United States) show PENCHUKOV had been using the “tank” nickname for online activity.

B. IVAN VIKTOROVICH KLEPIKOV, a/k/a “petr0vich”

42. Forensic examination of the INCOMEET SERVER showed that one of the nicknames used to communicate on the INCOMEET SERVER is “petr0vich.” The individual calling himself “petr0vich” has extensively discussed criminal activity over the INCOMEET SERVER. Among the messages he typed include discussion of the command and control servers through which stolen credentials are sent, discussions of the techniques for obtaining passwords and user authentication tokens, discussions of configuration files for the Zeus botnet, and discussion of “cashing”—that is, withdrawing money from—accounts.

43. As part of the Jabber instant messaging system, users are able to maintain a roster

of “friends,” whom they communicate with frequently. “petr0vich” includes theklutch@gmail.com among his friends. (Google users are able to send and receive Jabber messages, through the “Google Talk” service, using the same account names as their e-mail accounts). There is reason to believe that “theklutch@gmail.com” and “petr0vich” are the same person, because:

- a. I know from a grand jury subpoena served on Google, and also from log files located on the INCOMEET SERVER, that of the 21 unique Internet Protocol addresses used to log into the INCOMEET SERVER’s administrator account, three of them were also used to access the “theklutch@gmail.com” account: 195.244.5.4, 92.242.127.198, and 74.50.98.154. In particular, the 92.242.127.198 address was used 790 times to access the “theklutch@gmail.com” account. This strongly suggests that the person accessing the “theklutch@gmail.com” account is one of the persons controlling the INCOMEET SERVER.
- b. According to logs produced by Google pursuant to subpoena, the “theklutch@gmail.com” account is an actively used account, accessed several times per hour. The account was in heavy use during the times of known fraudulent bank transfers. Google lists the name associated with the account as “Ivan Klepikov,” the nickname as “petr0vich,” and the secondary e-mail as “petr0vich@ua.fm.” The account was created on November 24, 2004.
- c. The password on the INCOMEET SERVER for “petr0vich” is “johnklpkv,” a word that bears a strong similarity to “Ivan Klepikov,” the name used to register the “theklutch@gmail.com” account.

- d. In at least one chat, the user “deaduser” addressed “petr0vich” as “Ivan.” In that same chat, deaduser asked if petr0vich was at his home, offering to drive there. This suggests deaduser was familiar with petr0vich’s true identity, and that petr0vich’s first name is “Ivan.”

44. Information obtained from Ukrainian law enforcement reveals that there is an Ivan Viktorovich Klepikov who resides in Donetsk, Ukraine.

45. On January 14, 2010 at 8:24 AM, the IP address 92.242.127.198 was used to communicate with Google to access the email account of theklutch@gmail.com. Then, on January 14, 2010, at 8:24 AM the same IP address was used to contact the INCOMEET SERVER. As noted above, there is probable cause to believe that “theklutch@gmail.com” is one of petr0vich’s e-mail accounts.

46. On February 11, 2010 at 2:30 PM, the IP address 209.160.22.135 was used to communicate with Google to access the email account of theklutch@gmail.com. Then on February 11, 2010 at 2:31 PM, that same IP address was used to contact the INCOMEET SERVER.

C. ALEXEY DMITRIEVICH BRON, a/k/a “thehead”

47. On February 26, 2010, “thehead” stated in chat that BRON was his real name.

48. On December 26, 2009, “thehead” provided his email address in a chat message as alexey.bron@gmail.com.

D. ALEXEY TIKONOV, a/k/a “kusanagi”

49. On October 13, 2009, “kusanagi” used a Russian phone number during a chat.

That same phone number was found by FBI agents to be on a web page, sashatikonov.ru.

("Sasha" is a common diminutive name for "Alexey"). That page gives Alexey Tikonov's identifying information.

50. In chat, "kusanagi" has shared web links pointing to demo videos. Old WHOIS information for the name server hosting the domain names hosting those videos show they were registered by Alexey Tikonov in Tomsk, Russia.

E. YEVHEN KULIBABA, a/k/a "jonni"

51. Simon Williams, whom I know to be a Detective Sergeant for the Metropolitan Police, Police Central e-Crime Unit, has told me that on July 15, 2011, he was present in a U.K. court proceeding relating to U.K. charges against KULIBABA and KONOVALENKO during which the prosecutor referenced KULIBABA's online nickname as "jonni," and this online nickname was acknowledged by KULIBABA's defense counsel.

F. YURIY KONOVALENKO, a/k/a "jtk0"

52. Simon Williams, whom I know to be a Detective Sergeant for the Metropolitan Police, Police Central e-Crime Unit, has told me that on July 15, 2011, he was present in a U.K. court proceeding relating to U.K. charges against KULIBABA and KONOVALENKO during which the prosecutor referenced KONOVALENKO's online nickname as "jtk0," and this online nickname was acknowledged by KONOVALENKO's defense counsel.

THE RACKETEERING CONSPIRACY

53. From in or about May 2009, the exact date being unknown, and continuing to the present, in the District of Nebraska and elsewhere, VYACHESLAV IGOREVICH PENCHUKOV, IVAN VIKTORVICH KLEPIKOV, ALEXEY DMITRIEVICH BRON, ALEXEY TIKONOV, YEVHEN KULIBABA, YURIY KONOVALENKO, JOHN DOE #1,

JOHN DOE #2, and JOHN DOE #3 (hereinafter “DEFENDANTS”), each being a person employed by and associated with the Jabber Zeus Crew, an enterprise engaged in, and the activities of which affected, interstate and foreign commerce, together with others known and unknown, did knowingly and intentionally conspire to violate 18 U.S.C. § 1962(c), that is, to conduct and participate, directly and indirectly, in the conduct of the affairs of the enterprise through a pattern of racketeering activity, as defined in Sections 1961(1) and (5) of Title 18, United States Code, which pattern of racketeering activity consisted of multiple acts indictable under 18 U.S.C. § 1344 (bank fraud) and acts indictable under 18 U.S.C. § 1028 (identity theft).

54. It was part of the conspiracy that each defendant agreed that a conspirator would commit at least two acts of racketeering activity in the conduct of the affairs of the enterprise.

A. Manner and Means of the Conspiracy

55. It was part of the conspiracy that DEFENDANTS used computer intrusion, malicious software, and fraud to steal or attempt to steal millions of dollars from several bank accounts in the United States, and elsewhere.

56. It was further part of the conspiracy that DEFENDANTS installed, without authorization, malicious software known as “Zeus” or “Zbot” on Internet-connected computers without those computers’ owners’ authorization, thereby causing damage to those computers.

57. It was further part of the conspiracy that DEFENDANTS used that malicious software to capture bank account numbers, passwords, and other information necessary to log into online banking accounts.

58. It was further part of the conspiracy that DEFENDANTS used that captured information without authorization to falsely represent to banks that DEFENDANTS were

employees of the victims authorized to make transfers of funds from the victims' bank accounts.

59. It was further part of the conspiracy that DEFENDANTS used that captured information to cause banks to make unauthorized transfers of funds from the victims' bank accounts.

60. It was further part of the conspiracy that DEFENDANTS used as "money mules" residents of the United States who received funds transferred over the Automated Clearing House ("ACH") network or through other interstate wire systems from victims' bank accounts into the money mules' own bank accounts, and then withdrew some of those funds and wired the funds overseas to conspirators.

61. It was further part of the conspiracy that DEFENDANTS maintained Internet-connected computer servers, in the United States and elsewhere, to facilitate communication.

62. It was further part of the conspiracy that DEFENDANTS knowingly falsely registered a domain name and knowingly used that domain name in the course of the offense, in violation of 18 U.S.C. § 3559(g)(1).

B. Overt Acts

63. In furtherance of the conspiracy and to achieve the objectives thereof, at least one of the conspirators performed or caused to be performed at least one of the following overt acts, among others, in the District of Nebraska and elsewhere:

- a. On or about June 22, 2009, DEFENDANTS caused malicious software to be installed, without authorization, on a computer used by BULLITT COUNTY FISCAL COURT.
- b. On or about June 22, 2009, DEFENDANTS used stolen access information to

cause FIRST FEDERAL SAVINGS BANK to transfer funds out of a bank account belonging to BULLITT COUNTY FISCAL COURT and into one or more bank accounts designated by DEFENDANTS.

- c. On July 7, 2009, KLEPIKOV received a chat message from an alert messaging system which notifies members of the enterprise once a bank account has been compromised. The alert message was comprised of banking credential details concerning a bank account associated to FundsXpress.
- d. On July 7, 2009, "mricq" received a chat message from an alert messaging system which notifies members of the enterprise once a bank account has been compromised. The alert message was comprised of banking credential details concerning a bank account associated to FundsXpress.
- e. On July 8, 2009, BRON received a chat message from PENCHUKOV which included details of bank account associated to Wells Fargo. The message contained information concerning a victim bank account, user credentials and bank account numbers.
- f. On July 8, 2009, "lucky12345" sent a chat message to PENCHUKOV which included details of a victim bank account belonging to All Things Pawssbile. The message contained account and company identification information.
- g. On July 8, 2009, "lucky12345" sent a chat message to PENCHUKOV which included details of a victim bank account belonging to Arm-Strong Fitness Inc. The message contained account and company identification information.
- h. On or about July 8, 2009, PENCHUKOV transmitted login credentials for an employee of TOWN OF EGREMONT to JOHN DOE #3.

- i. On or about July 8, 2009, DEFENDANTS caused malicious software to be installed, without authorization, on a computer used by ODAT LLC.
- j. On or about July 8, 2009, KULIBABA sent PENCHUKOV online messages identifying bank accounts of victims and providing bank account information for money mules to receive funds stolen from victims.
- k. On or about July 8, 2009, DEFENDANTS used stolen access information to attempt to cause UNION BANKSHARES CORPORATION to transfer funds out of a bank account belonging to ODAT LLC and into one or more bank accounts designated by DEFENDANTS.
- l. On July 9, 2009, KULIBABA received a chat message from PENCHUKOV which included details of a transfer from a victim bank account belonging to ODAT LLC. The message included the amount to be transferred and the money mule name and account to which the money was deposited.
- m. On July 9, 2009, KULIBABA received a chat message from PENCHUKOV which included details of a transfer from a victim bank account belonging to Williamsburg Millwork Corp. The message included the amount to be transferred and the money mule names and account to which the money was deposited.
- n. On or about July 12 and 13, 2009, PENCHUKOV, JOHN DOE #2, and another individual exchanged online messages about unauthorized withdrawals they had made from accounts owned by BULLITT COUNTY FISCAL COURT.
- o. On or about July 15, 2009, JOHN DOE #3 received an online message

containing login credentials for an employee of TOWN OF EGREMONT and a link to a website of SALISBURY BANK & TRUST.

- p. On July 24, 2009, "mricq" received a chat message from an alert messaging system which notifies members of the enterprise once a bank account has been compromised. The alert message was comprised of banking credential details concerning a bank account associated to Wachovia Bank.
- q. On or about July 28, 2009, DEFENDANTS caused malicious software to be installed, without authorization, on a computer used by DOLL DISTRIBUTING.
- r. On or about July 28, 2009, PENCHUKOV sent an online message to a conspirator regarding transfers of funds from a bank account belonging to DOLL DISTRIBUTING.
- s. On or about July 29, 2009, DEFENDANTS used stolen access information to attempt to cause FIRST NATIONAL BANK OF OMAHA to transfer funds out of a bank account belonging to DOLL DISTRIBUTING and into one or more bank accounts designated by DEFENDANTS.
- t. On or about July 29, 2009, DEFENDANTS caused malicious software to be installed, without authorization, on a computer used by TOWN OF EGREMONT.
- u. On or about July 29, 2009, DEFENDANTS used stolen access information to cause SALISBURY BANK & TRUST to transfer funds out of a bank account belonging to TOWN OF EGREMONT and into one or more bank accounts designated by DEFENDANTS.

- v. On or about July 30, 2009, JOHN DOE #3 sent JOHN DOE #2 an online message about the TOWN OF EGREMONT bank account.
- w. On or about July 30, 2009, DEFENDANTS used stolen access information to cause SALISBURY BANK & TRUST to transfer funds out of a bank account belonging to TOWN OF EGREMONT and into one or more bank accounts designated by DEFENDANTS.
- x. On or about August 12, 2009, DEFENDANTS caused malicious software to be installed, without authorization, on a computer used by FRANCISCAN SISTERS OF CHICAGO.
- y. On or about August 12, 2009, DEFENDANTS used stolen access information to cause BANK OF AMERICA to transfer funds out of a bank account belonging to FRANCISCAN SISTERS OF CHICAGO and into one or more bank accounts designated by DEFENDANTS.
- z. On or about August 13, 2009, PENCHUKOV sent an online message to JOHN DOE #2 listing recipients and amounts of funds transferred from a bank account belonging to FRANCISCAN SISTERS OF CHICAGO.
- aa. On or about August 25, 2009, DEFENDANTS caused malicious software to be installed, without authorization, on a computer used by UNITED DAIRY, INC.
- bb. On or about August 26, 2009, DEFENDANTS used stolen access information to cause KEY BANK to transfer funds out of a bank account belonging to UNITED DAIRY, INC. and into one or more bank accounts designated by DEFENDANTS.

- cc. On or about August 28, 2009, PENCHUKOV and JOHN DOE #3 received an online message containing login credentials for an employee of UNITED DAIRY, INC.
- dd. On August 28, 2009, “aqua” sent a chat message to PENCHUKOV which included details of five victim bank accounts. The message contained victim names, bank account and routing information.
- ee. On September 1, 2009, “aqua” received a chat message from PENCHUKOV which included details of multiple transfers from a victim bank account belonging to Enoch Manufacturing Company. The message included the names, bank account details and deposit amounts of nine money mules.
- ff. On September 2, 2009, PENCHUKOV sent a chat message to an associate known as “fanesso” which included the banking information of the victim The Escrow Source. The details included in the message were banking credentials of The Escrow Source, beneficiary information and total amount to be deposited.
- gg. On September 23, 2009, KLEPIKOV received a chat message from PENCHUKOV which included details of a bank account associated to the Nashville Citizens Bank. The message contained client banking login information.
- hh. On September 23, 2009, BRON received a chat message from PENCHUKOV which included details of a bank account associated to Chase Bank. The message contained information concerning a victim bank account and bank account numbers.

- ii. On or about September 28, 2009, DEFENDANTS caused malicious software to be installed, without authorization, on a computer used by PARAGO, INC.
- jj. On or about September 28, 2009, DEFENDANTS used stolen access information to attempt to cause FIRST NATIONAL BANK OF OMAHA to transfer funds out of a bank account belonging to PARAGO, INC. and into one or more bank accounts designated by DEFENDANTS.
- kk. On or about September 28, 2009, PENCHUKOV transmitted login credentials for an employee of PARAGO, INC. to JOHN DOE #3.
- ll. On November 25, 2009, TIKONOV received a chat message from PENCHUKOV which included details of bank account associated to Citizens Bank. The message contained information concerning a victim bank account and banking credentials.
- mm. On December 3, 2009, KONOVALENKO sent a chat message to KULIBABA which included the details of eight victim bank accounts. The message included the bank website URL (uniform resource locator), name associated to the accounts and login credentials to access each account.
- nn. On February 4, 2010, TIKONOV received a chat message from PENCHUKOV which included detail of a bank account associated of City National Bank. The message contained information concerning a victim bank account and banking credentials.
- oo. On or about March 3, 2010, DEFENDANTS caused malicious software to be installed, without authorization, on a computer used by HUSKER AG, LLC.
- pp. On or about March 3, 2010, DEFENDANTS used stolen access information to

attempt to cause UNION BANK AND TRUST to transfer funds out of a bank account belonging to HUSKER AG, LLC and into one or more bank accounts designated by DEFENDANTS.

qq. On or about March 3, 2010, PENCHUKOV, TIKONOV, and JOHN DOE #3 received a message containing stolen access credentials for an employee of HUSKER AG, LLC.

rr. On or about March 8, 2010, KONOVALENKO sent KULIBABA an online message regarding how much money he was making operating money mules for PENCHUKOV.

CONCLUSION

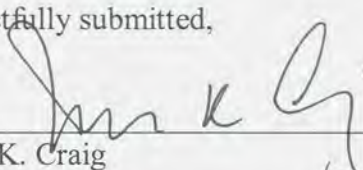
64. Based on the foregoing, I submit there is probable cause to believe that from in or about May 2009, and continuing to the present, in the District of Nebraska and elsewhere, VYACHESLAV IGOREVICH PENCHUKOV, IVAN VIKTORVICH KLEPIKOV, ALEXEY DMITRIEVICH BRON, ALEXEY TIKONOV, YEVHEN KULIBABA, YURIY KONOVALENKO, JOHN DOE #1, JOHN DOE #2, and JOHN DOE #3 (hereinafter "DEFENDANTS"), each being a person employed by and associated with the Jabber Zeus Crew, an enterprise engaged in, and the activities of which affected, interstate and foreign commerce, together with others known and unknown, did knowingly and intentionally conspire to violate 18 U.S.C. § 1962(c), that is, to conduct and participate, directly and indirectly, in the conduct of the affairs of the enterprise through a pattern of racketeering activity, as defined in 18 U.S.C. §§ 1961(1) & (5), which pattern of racketeering activity consisted of multiple acts indictable under 18 U.S.C. § 1344 (bank fraud) and 18 U.S.C. § 1028 (identity theft). It was a further part of the conspiracy that each defendant agreed that a conspirator would commit at least two acts of

racketeering activity in the conduct of the affairs of the enterprise.

REQUEST FOR SEALING

65. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and complaint. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits via the Internet, and disseminate them to other online criminals as they deem appropriate, e.g., by posting them publicly online. The crimes discussed in this affidavit have already been the subject of media attention, and there is a danger that the information in this affidavit could be further disseminated by journalists. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,



James K. Craig
Special Agent
FBI

Subscribed and sworn to before me
on July 13, 2012.



UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Offense description

From in or about May 2009, and continuing to the present, in the District of Nebraska and elsewhere, VYACHESLAV IGOREVICH PENCHUKOV, IVAN VIKTORVICH KLEPIKOV, ALEXEY DMITRIEVICH BRON, ALEXEY TIKONOV, YEVHEN KULIBABA, YURIY KONOVALENKO, JOHN DOE #1, JOHN DOE #2, and JOHN DOE #3 (hereinafter “DEFENDANTS”), each being a person employed by and associated with the Jabber Zeus Crew, an enterprise engaged in, and the activities of which affected, interstate and foreign commerce, together with others known and unknown, did knowingly and intentionally conspire to violate 18 U.S.C. § 1962(c), that is, to conduct and participate, directly and indirectly, in the conduct of the affairs of the enterprise through a pattern of racketeering activity, as defined in 18 U.S.C. §§ 1961(1) & (5), which pattern of racketeering activity consisted of multiple acts indictable under 18 U.S.C. § 1344 (bank fraud) and 18 U.S.C. § 1028 (identity theft). It was a further part of the conspiracy that each defendant agreed that a conspirator would commit at least two acts of racketeering activity in the conduct of the affairs of the enterprise.

In violation of Section 1962(d) of Title 18 of the United States Code.